PATENT ABSTRACTS OF JAPAN

(11)Publication number :	**2000-172548**
(43)Date of publication of application :	**23.06.2000**

(51)Int.Cl.	**G06F 12/00** **G06F 3/06** **G06F 12/14** **H04L 9/06**

(21)Application number :	**10-352349**	(71)Applicant :	**NIPPON TELEGR & TELEPH CORP <NTT>**
(22)Date of filing :	**11.12.1998**	(72)Inventor :	**HORIOKA TSUTOMU** **NAGATA TAKAOKI** **WATABE YASUHIKO** **SONEHARA NOBORU**

(54) **ELECTRONIC DATA MANAGEMENT METHOD AND DEVICE AND RECORDING MEDIUM OF ELECTRONIC DATA MANAGEMENT PROGRAM**

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a means which inhibits a key against a wrong user to discriminate the electronic data to be protected from other data and then prevents the wrong user from recognizing the location of the electronic data to be protected.

SOLUTION: When the electronic data are stored, an electronic data dividing part 12 divides the electronic data which are handled as a single source electronic file into at least two or more pieces. An electronic data enciphering part 13 enciphers the divided electronic data, and a divided data management part 14 stores the enciphered electronic data 19 in an electronic data storing part 15 as divided files and also manages the divided data management information 18 on the storage of the divided files. When the electronic data are acquired, the part 14 reads out the data 19 based on the information 18. Then an electronic data decoding part 16 decodes the data 19 and an electronic data reconfiguring part 17 integrates the decoded data 19 to reconfigure them into the original electronic data.

LEGAL STATUS

[Date of request for examination]	22.12.2000
[Date of sending the examiner's decision of rejection]	06.09.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

[Claim(s)]

[Claim 1] In the electronic data control approach of managing the electronic data processed on a calculating machine While accumulating the process in which a series of electronic data to accumulate is inputted, the process which enciphers said electronic data, the process in which said encryption data are divided into at least two or more division files, and said division file The process in which the management information about the are recording is memorized, and the process which acquires said division file based on said management information, The electronic data control approach characterized by having the process which unifies the electronic data of said acquired division file, and is reconfigurated to the encryption data before said division, the process which decodes said reconfigurated electronic data, and the process which outputs said decoded electronic data.

[Claim 2] In the electronic data control approach of managing the electronic data processed on a calculating machine The process in which a series of electronic data to accumulate is inputted, and the process in which said electronic data is divided into at least two or more electronic data, While storing the process which enciphers said divided electronic data for every division data, and said enciphered division data as a division file The process in which the management information about the are recording is memorized, and the process which acquires said division file based on said management information, The electronic data control approach characterized by having the process which decodes the electronic data of said acquired division file for every division file, the process which unifies the decode data for said every division file, and is reconfigurated to the original electronic data, and the process which outputs said reconfigurated electronic data.

[Claim 3] In the electronic data control equipment which manages the electronic data processed on a calculating machine One original electronic file, a means to output and input the electronic data treated, and a means to encipher the electronic data inputted for are recording, While accumulating a means to divide said encryption data into at least two or more division files, and said division file A means to manage the management information about the are recording, and a means to acquire said division file which originates in said Hara electronic file based on said management information, Electronic data control equipment characterized by having a means to unify and reconfigurate the electronic data of said acquired division file, and a means to decode said reconfigurated electronic data.

[Claim 4] In the electronic data control equipment which manages the electronic data processed on a calculating machine One original electronic file, a means to output and input the electronic data treated, and a means to divide into at least two or more electronic data the electronic data inputted for are recording, While storing a means to encipher said divided electronic data for every division data, and said enciphered division data, as a division file A means to manage the management information about the are recording, and a means to acquire said division file which originates in said Hara electronic file based on said management information, Electronic data control equipment characterized by having a means to decode the electronic data of said acquired division file for every division file, and a means to unify the decode data for said every division file, and to reconfigurate to the original electronic data.

[Claim 5] The processing which is the record medium which recorded the program for managing the electronic data processed on a calculating machine, and enciphers the electronic data treated as one original electronic file, While accumulating said division file with the processing which divides said encryption data into at least two or more division files The processing which memorizes the management information about the are recording, and the processing which acquires said division file which originates in said Hara electronic file based on said management information, The electronic data management record medium characterized by recording the program which makes a calculating machine perform processing which unifies and reconfigurates the electronic data of said acquired division file, and processing which decodes said reconfigurated electronic data.

[Claim 6] The processing which divides into at least two or more electronic data the electronic data which is the record medium which recorded the program for managing the electronic data processed on a calculating machine, and is treated as one original electronic file, While storing said enciphered division data as a division file with the processing which enciphers said divided electronic data for every division data The processing which memorizes the management information about the are recording, and the processing which acquires said division file which originates in said Hara electronic file based on said management information, The electronic data management record medium characterized by recording the program which makes a calculating machine perform processing which decodes the electronic data of said acquired division file for every division file, and processing which unifies the decode data for said every division file, and is reconfigurated to the original electronic data.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the electronic data control approach and electronic data control equipment for managing safely the electronic data accumulated on the computer.

[0002]

[Description of the Prior Art] Usually, electronic data is stored for every file as a set of 1 lump, and is managed on a computer. In management, a name and the date and time of creation are given for every file, and the data aggregate can be distinguished now from other things. Although only the just user to the electronic data should be available in the electronic data, when persons other than the user accepted to be just originally use the computer with which the electronic data was memorized, if there is no device, no use of the electronic data can be restricted. As the cure, it considered enciphering electronic data for every file. However, in the management for every file, the key for distinguishing the electronic data and other electronic data for an inaccurate user will be left behind.

[0003]

[Problem(s) to be Solved by the Invention] The purpose of this invention is by offering the means which stops the key which distinguishes the electronic data which serves as a candidate for protection to an inaccurate user from other electronic data to bar recognition of the whereabouts of the electronic data used as the candidate for protection.

[0004]

[Means for Solving the Problem] In management of electronic data, at the time of are recording of electronic data, the electronic data stored in one original electronic file is enciphered, the encryption data is divided into at least two or more division files, and the attribute information on those division file and its original electronic file and encryption information are memorized. At the time of use (acquisition) of electronic data, the division file originating in said Hara electronic file is acquired, the electronic data of the acquired division file is unified, and the electronic data integrated is decoded.

[0005] Or the electronic data stored in one original electronic file at the time of are recording of electronic data is divided into at least two or more division files, the electronic data stored in the division file is enciphered for every division file, and the attribute information on those division file and its original electronic file and encryption information are memorized. At the time of use (acquisition) of electronic data, the division file originating in said Hara electronic file is acquired, the encryption data in a division file are decoded for every division file, those decryption data are unified, and electronic data is made available.

[0006] A program for a computer to realize each above processing means is storable in suitable record media, such as portable medium memory which a computer can read, semiconductor memory, and a hard disk.

[0007]

[Embodiment of the Invention] [Gestalt of the 1st operation] The example in the case of dividing a series of electronic data in a computer top as a gestalt of operation of the 1st of this invention, enciphering, respectively and managing the divided electronic data is explained.

[0008] Drawing 1 is drawing showing the outline configuration of the electronic data control equipment in the gestalt of the 1st operation. the inside of drawing, and 10 -- electronic data control equipment and 11 -- the electronic data I/O section and 12 -- the electronic data division section and 13 -- the electronic data encryption section and 14 -- in the electronic data decode section and 17, the electronic data restructuring section and 18 express division data control information, and, as for the division data control section and 15, 19 expresses [the electronic data accumulation section and 16] encryption electronic data.

[0009] When accumulating electronic data, through the electronic data I/O section 11, data are set to reception, and electronic data control equipment 10 sets the received data in the electronic data division section 12, and divides them into data without functionality. Furthermore, it enciphers in the electronic data encryption section 13, and the divided data is sent to the division data control section 14. In the division data control section 14, said enciphered data (encryption electronic data 19) are stored in the electronic data accumulation section 15, and a preservation location and the information about division are managed as division data control information 18.

[0010] However, the data divided in the electronic data division section 12 are the magnitude which cannot grasp the contents of data from one of the divided data of the, and are data which cannot guess relation with other data.

[0011] Generally as the approach of encryption, various things are proposed from the former, and what kind of encryption approach may be used in the encryption in the electronic data encryption section 13. For example, a key is easily manageable if a common key encryption system is used. A common key encryption system is a cipher system the key to encipher and whose key to decode are the same keys. On the other hand, when applying a public key cryptosystem to this method, encryption and decode are attained by managing two keys. However, generally, since a public key cryptosystem needs remarkable computation time, it needs to shorten the time amount which count takes using the computer of high performance.

[0012] When returning division data, the encryption electronic data 19 accumulated in the electronic data accumulation section 15 from the division data control information 18 is elected. Next, the encryption electronic data 19 is decoded in the electronic data decode section 16, and the electronic data divided in the electronic data restructuring section 17 is unified as one electronic data, and is reconfigurated. The reconfigurated electronic data is sent out through the electronic data I/O section 11.

[0013] Drawing 2 is the processing flow chart of the electronic data accumulation processing by the gestalt of operation of the 1st of this invention. In accumulating electronic data, it enciphers the electronic data which divided electronic data by the electronic data division section 12 first (step S11), and then was divided by the electronic data encryption section 13 (step S12). By the division data control section 14, division data control information 18 ** about the are recording location of the enciphered electronic data is saved (step S13), and the encryption electronic data 19 divided into the electronic data accumulation section 15 is accumulated (step S14).

[0014] Drawing 3 is the processing flow chart of the electronic data acquisition processing by the gestalt of operation of the 1st of this invention. In acquiring the electronic data accumulated, the division data control information 18 about the are recording location of the electronic data divided and accumulated is acquired first (step S21), and it acquires the encryption electronic data 19 divided based on the division data control information 18 (step S22). Next, the encryption electronic data 19 is decoded by the electronic data decode section 16 (step S23), and electronic data is unified by the electronic data restructuring section 17, and it reconfigurates (step S24). By this, electronic data is made available.

[0015] Although the enciphered electronic data was divided and the example to manage was shown by this example, when enciphering to each data after dividing electronic data in this way, it is also possible to use the same cryptographic key and to manage with one key to each divided data. Moreover, you may encipher by changing and scrambling the order of a data list, without using a cryptographic key etc.

[0016] [Gestalt of the 2nd operation] As a gestalt of the 2nd operation, the electronic data enciphered on the computer is divided into below, and the example in the case of managing the divided electronic data is explained to it. Drawing 4 is drawing showing the outline configuration of the electronic data control equipment in the gestalt of the 2nd operation. the inside of drawing, and 20 -- electronic data control equipment and 21 -- the electronic data I/O section and 22 -- the electronic data encryption section and 23 -- the electronic data division section and 24 -- in the electronic data restructuring section and 27, the electronic data decode section and 28 express division data control information, and, as for the division data control section and 25, 29 expresses [the electronic data accumulation section and 26] encryption electronic data.

[0017] The electronic data I/O section 21 outputs and inputs the electronic data to accumulate. In application, using this equipment, preservation and when acquiring, the data exchange with application is performed through the electronic data I/O section 21.

[0018] In the electronic data encryption section 22, the electronic data received in the electronic data I/O section 21 is enciphered. It does not ask about the approach of enciphering. In the electronic data division section 23, the electronic data enciphered by the electronic data encryption section 22 is divided. However, in the electronic data encryption section 22, as the encryption approach, when the block cipher is used, as shown in drawing 5 , since it is enciphered by a certain the settlement (block data 32, 33, 34, and 35) of every and electronic data 31 is treated as one encryption electronic data 36, it is performed in the form where each block data is divided.

[0019] In the division data control section 24, the information which shows where it accumulates is described to the division data control information 28, and the encryption electronic data 29 is accumulated in the electronic data accumulation section 25.

[0020] When taking out electronic data, the encryption electronic data 29 accumulated in the electronic data accumulation section 25 is taken out based on the division data control information 28. In the electronic data restructuring section 26, after reconfigurating the encryption electronic data 29 acquired based on the division data control information 28, in the electronic data decode section 27, it decodes to the original electronic data.

[0021] Drawing 6 is the processing flow chart of the electronic data accumulation processing by the gestalt of operation of the 2nd of this invention. An input of the electronic data accumulated by the electronic data I/O section 21 divides the electronic data which enciphered electronic data by the electronic data encryption section 22 first (step S41), and was enciphered by the electronic data division section 23 (step S42). Next, the division information and are recording information on electronic data are saved as division data control information 28 by the division data control section 24 (step S43), and the encryption electronic data 29 is accumulated by the electronic data accumulation section 25 (step S44).

[0022] Drawing 7 is the processing flow chart of the electronic data acquisition processing by the gestalt of operation of the 2nd of this invention. First, the division data control information 28 which shows how the demanded electronic data is accumulated is acquired (step S51), and the encryption electronic data 29 is acquired based on the division data control information 28 (step S52). Next, the acquired encryption electronic data 29 is unified and reconfigurated based on the division data control information 28 (step S53), and it decodes to the original electronic data before division and encryption (step S54).

[0023] [Example of application] Next, the example in the case of dividing and managing the electronic data (henceforth a file) created by application (editor) as an example of application of this invention is explained. This example is an example at the time of using a text file as a file using the editor into which text data, such as a program, are edited as application.

[0024] File management with each means shown in drawing 1 or drawing 2 shall be registered into the editor. Although the registration to an editor is premised on the plug-in system started as a helper program only for editors, it cannot be overemphasized that the demon (program is always moving) program method which resides in a calculating machine permanently may be used. Drawing 8 (A) shows the example of a program configuration in a plug-in system, and drawing 8 (B) shows the example of a program configuration in the case of a demon program method. In the case of the demon program method especially shown in drawing 8 (B), it is possible to also receive the file preservation request from programs other than editor program 43.

[0025] When saving the electronic data of the edited text, an editor requests file preservation processing from file management. File management investigates whether the requested file exists from the file control table currently held beforehand, and when it does not exist, it registers the file management information into a file control table newly. This file control table is a table holding the division data control information 18 on drawing 1 , or the division data control information 28 on drawing 2 .

[0026] The example of the division data control information managed with a file control table by drawing 9 is shown. As a component of a file control table, there are a file name used as the candidate for preservation, a cryptographic key which enciphers a file, the file number of partitions, a divided file name. As shown in drawing 10 , by specifying preservation places, such as an absolute path, as a file name and coincidence, it is made to distribute on a network and the file name divided and saved can also be saved.

[0027] When the file is already registered, the variable based on a file name is created and a file is enciphered as a cryptographic key. When generating a cryptographic key from a file name, it is also possible to use a general random-number generating function and to generate a cryptographic key directly from a file name. For example, it is also possible to change a file name into an ASCII code, to extract the 1st bit of each alphabetic character, and to consider as a new character code. Since it is one character in 1 byte, an ASCII code deletes surplus data, when many, and when insufficient, it can be complemented with 0. Moreover, when the head of a file name is the same name, it becomes possible by taking an exclusive OR with the time of preservation etc. to classify.

[0028] Next, the enciphered file is divided. Since it is enciphered as a mass of data for every bitwise of a certain when a block cipher is used for encryption, there is a possibility that a specific bit pattern may be detected depending on the approach of encryption. In this case, it is necessary to divide so that the original data may not understand some.

[0029] For example, to the enciphered data, it extracts 1 bit at a time for every encryption block unit, and considers as one file. 56 files will be created when enciphering by 56 bitwises.

[0030] If the data used as the candidate for encryption are an ASCII code when enciphering after dividing, since it is expressed per 1 byte, each alphabetic character is extracted for every bit of each code (alphabetic character), and is saved as one file. The 1st bit of each alphabetic character is treated as one division file. In this case, since it is 1 byte = 8 bits, eight division files will be generated.

[0031] The example of encryption by conversion of an alphabetic character data bit train is shown in drawing 11 . "10110110" etc. expresses an alphabetic character (character) by the bit string. They are the example of the electronic data with which drawing 11 (A) serves as a candidate for are recording, and the example of the electronic data with which drawing 11 (B) was divided and enciphered. In this example, the head bit of each alphabetic character of electronic data 50 is extracted in order, and alphabetic character bit string 10110011 -- which consists of that bit [1st] data aggregate is considered as one division file 51. By performing this to each bit, the division files 51-58 which consist of each data aggregate from the 1st bit to the 8th bit are generated.

[0032] Next, the file name which can guess that it was one file mutually is attached to the divided data, it saves at a store, and the information is recorded on a file control table. A program may perform naming of a file to arbitration from the number of partitions or a file name.

[0033] At the time of the electronic data acquisition at the time of using electronic data, file management extracts the file name of division data from a file control table, and acquires each division file. Next, the cryptographic key generated based on the file name is acquired, and encryption electronic data is decoded. Furthermore, according to the divided approach, it restores to the original data list and a file is reconfigurated.

[0034] In this example, file management performs management of the above-mentioned cryptographic key, and it is used only within this program. That is, this cryptographic key is not told outside by the request from other applications etc. When a program is completed, using a cryptographic key, the program itself enciphers including a cryptographic key and it saves as a file the file control table shown in drawing 9 .

[0035] In performing preservation depending on application, the plug-in system is suitable, but when the program configuration of the above file management also enables use from other applications or service, it can use this method simply by making it the demon program method. In this case, in order to prevent access from an inaccurate user (or application and service), it cannot be overemphasized that it is necessary use the existing security methods, such as user authentication, and to prove the justification to a file access.

[0036]

[Effect of the Invention] As explained above, according to this invention, men other than a just electronic data user become possible [making difficult acquisition of the electronic data acquired easily conventionally] by dividing electronic data beforehand and managing it on the computer.

[0037] Moreover, it becomes difficult to return the electronic data enciphered and divided by enciphering the electronic data to divide beforehand.

[0038] Furthermore, it becomes difficult to return the electronic data divided and enciphered by enciphering for every divided electronic data.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the outline configuration of the electronic data control equipment in the gestalt of operation of the 1st of this invention.

[Drawing 2] It is the processing flow chart of the electronic data accumulation processing by the gestalt of the 1st operation.

[Drawing 3] It is the processing flow chart of the electronic data acquisition processing by the gestalt of the 1st operation.

[Drawing 4] It is drawing showing the outline configuration of the electronic data control equipment in the gestalt of operation of the 2nd of this invention.

[Drawing 5] It is drawing explaining the example of a block cipher.

[Drawing 6] It is the processing flow chart of the electronic data accumulation processing by the gestalt of the 2nd operation.

[Drawing 7] It is the processing flow chart of the electronic data acquisition processing by the gestalt of the 2nd operation.

[Drawing 8] It is drawing for explaining the example of cooperation with application.

[Drawing 9] It is drawing showing the example of division data control information (file control table).

[Drawing 10] It is drawing showing the example of the name at the time of division file preservation.

[Drawing 11] It is drawing showing the example of encryption by conversion of an alphabetic character data bit train.

[Description of Notations]

10 20 Electronic data control equipment
11 21 Electronic data I/O section
12 23 Electronic data division section
13 22 Electronic data encryption section
14 24 Division data control section
15 25 Electronic data accumulation section
16 27 Electronic data decode section
17 26 Electronic data restructuring section
18 28 Division data control information
19 29 Encryption electronic data